new era.
TECHNOLOGY

New Era Technology, Inc. Encryption Policy

Classification: Public

Encryption Statement

New Era Technology, Inc., and its subsidiaries (collectively the “Company” or “New Era”) is committed to upholding the rules for acceptable use of encryption technologies relating to New Era Technology Information Resources.

We expect this policy to be upheld by all employees, (permanent, temporary, or contracted), including executives, officers, and directors of New Era.

Contents

1. Terms and Definitions

Term / Acronym	Definition / Meaning
"data"	are items of information.
"cryptography"	means the process of encrypting and decrypting data.
"information"	Information is processed, organized, and structured data. It provides context for data and enables decision-making processes. Information can be collected, used, stored, reported, or presented in any format, on any medium.
"information resource"	means information and related resources, such as personnel, equipment, funds, and information technology.
"staff", "users", "personnel"	means those who are employed by New Era Technology on a full-time, part-time, or temporary basis; those who access and / or utilize New Era Technology's information resources, including, but not limited to employees, contractors, interns, third and external parties.
"we", "our", "New Era", or "New Era Technology"	refers to New Era Technology, Inc., and its subsidiaries.

2. Scope

This Policy covers all New Era Technology's information, systems, networks, and other information assets to ensure adequate controls are in place to ensure the confidentiality, integrity and availability of our data. These critical assets must be managed and controlled to protect our company from loss due to misuse, disclosure, fraud, or destruction.

This Policy applies to all New Era Technology's remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to New Era's electronic systems, information, software, and/or hardware.

This Policy also pertains to all systems, networks, and users connected to New Era Technology resources through any means, including but not limited to local access, leased lines, wireless access points, or any other telecommunications device, through either private or public networks. It also applies to all third-party local and remote connections as well as non-company assets involved in the storage, processing, or transmission of New Era Technology's information or data.

The terms set out in this Policy work in conjunction with, and do not replace, amend, or supplement any terms or conditions of employment stated in any collective bargaining agreements and/or employment contracts.

This Policy is not intended to restrict communications or actions protected or required by regional/local laws and regulations.

Relationship to Local/Regional Policies

This Encryption Policy is New Era's corporate policy. New Era Technology business units and/or subsidiaries may complement this with a local/regional policy however, this Policy shall always be the minimum standard; a local/regional policy may augment, or increase the standards, but shall not detract from the New Era Technology encryption standards.

If any additional acceptable use policies are developed, Director of Governance, Risk and Compliance (GRC) must review and approve prior to release and publication.

3. Roles and Responsibilities

The Director of Governance, Risk and Compliance (GRC) and the Chief Technology Officer are responsible for the New Era Technology Security framework and its associated policies.

This Policy is reviewed annually by members of GRC. Any changes to this Policy will be approved by New Era Technology's Chief Technology Officer and Director of Governance, Risk, and Compliance prior to its release.

Suggestions for change to this Policy should be reported to GRC@neweratech.com.

The Information Technology (IT) departments and / or asset owners are responsible for managing encryption activities for New Era Technology.

All employees, contractors and third parties who access New Era Technology's information must abide by this and associated policies.

Technology owners are responsible for technical standards applicable to their operating environments and domains.

Line managers have day–to–day responsibility for this policy, and employees should refer any questions about this policy to them in the first instance.

In line with their applicable solutions groups, New Era's business units shall develop, disseminate, and maintain formal, documented processes and/or procedures to facilitate the implementation of this Policy and, where applicable, any local/regional acceptable use policies.

The processes and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, and/or standards.

4. Policy

Overview

1. New Era Technology's Chief Technology Officer (CTO), or delegate must approve all encryption technologies and techniques used by New Era. Cryptographic solutions are classified into cryptographic components and cryptographic services realizing the following features:
    a. Authentication.
    b. Message authentication (code signature, message signature).
    c. Encryption (Encryption in Transit, Encryption at Rest, Encryption in Use).
    d. Key management and key protection certificate management.
2. New Era Technology IT Management is responsible for distributing and managing all encryption keys.
3. All use of encryption technology should be managed in a manner that permits properly designated New Era Technology personnel to promptly access all data, including for investigation and business continuity.
4. Only encryption technologies approved, managed, and distributed by New Era Technology IT may be used in connection with New Era Technology Information Resources.
5. New Era Technology IT Management will create the New Era Technology Encryption Standards, which must include, at a minimum:
    a. The type, strength, and quality of the encryption algorithm that are required for various levels of protection.
    b. Key lifecycle management, including generation, storing, archiving, retrieving, distributing, retiring, and destroying keys.
6. All New Era Technology information classified as Confidential must be encrypted when:
    a. Transferred electronically over public networks.
    b. Stored on mobile storage devices.
    c. Stored on laptops or other mobile computing devices.
    d. At rest.
7. The use of proprietary encryption algorithms is not permitted unless approved by New Era Technology's CTO, or delegate.
8. Data transfer without encryption must be approved by New Era Technology's CTO, or delegate.
9. Prior to any data (encrypted or not) being transferred or stored outside of New Era approved systems must be approved by New Era Technology's CTO, or delegate.

Cryptographic Controls

This section covers the use of cryptography to encrypt confidential (sensitive) data.

1. Cryptographic controls must be utilized for sensitive information classified by our company as Confidential including, but not limited to:
    a. Personally Identifiable Information (PII).
    b. Protected Health Information (PHI).
    c. Credit card numbers.
    d. Passwords.
    e. Intellectual property.
    f. Budget or contract proposals.
    g. Legal correspondence.
    h. Research and development information.
2. The New Era Technology CTO, or delegate must authorize all encryption mechanisms utilized by New Era Technology.
3. Users must not attempt to utilize any form of cryptography, including, but not limited to, encryption, digital signatures, and digital certificates, which have not been approved and installed/implemented by New Era Technology’s CTO, or delegate.
4. All encryption mechanisms must meet relevant regulatory and legal requirements, including any import/export requirements and the use of cryptography in other countries.

Key Management

1. All encryption keys must be managed using a commercially available key management system.
2. The key management system must ensure that all encryption keys are secured, and there is limited access to New Era Technology authorized personnel.
3. Master keys and privileged access to the key management system must be granted to at least two administrators.
4. Keys generated by the key management system must not be easily discernible and easy to guess.
5. When keys are transmitted to third-party users, the encryption key must be transmitted over a different communication channel than the data that has been encrypted.
6. All key recovery operations must be authorized, and the key management system must log all activities.
7. New Era Technology IT Management must periodically review all logged activities (at least annually).

Network Encryption

1. All sensitive information classified by New Era as Confidential (including, but not limited to, PII, PHI, credit card numbers, passwords, and research and development information) must be encrypted when transmitted outside New Era.
    a. This includes the transmission of information via email or other communication channels.
2. Remote management activities, such as contractors accessing a New Era network remotely, must consistently employ session encryption.

Storage (Data-at-Rest) Encryption

1. All sensitive information classified by New Era as Confidential, including, but not limited to PII, PHI, credit card numbers, and passwords, must be encrypted.
2. When feasible, hardware encryption must be utilized over software encryption.
3. It is New Era Technology's policy is to use laptops and desktops with encrypted hard drives - or use a built-in disk encryption feature.

5. Compliance, Monitoring and Enforcement

This Policy is intended for all New Era businesses, in all countries.

New Era Technology seeks to proactively prevent and mitigate instances of non–compliance with this Policy.

Compliance is measured through various methods, including but not limited to risk assessments, business tool reports, internal and external audits, etc.

Any breaches or concerns, including ethical concerns or potential breaches in our commitment to information and data protection standards, should be reported as soon as possible through our Whistleblowing Policy.

Any need for improvements will be applied as soon as possible. Employees are encouraged to offer their feedback on this Policy if they have any suggestions for how it may be improved. Feedback of this nature should be addressed to GRC@neweratech.com.

Any exception to this Policy must be approved by the New Era Technology's Chief Technology Officer, or delegate and / or Director of Governance, Risk, and Compliance in advance.

Personnel found to have intentionally violated this Policy may be subject to disciplinary action, up to and including termination of employment and other penalties as set forth herein. New Era Technology reserves the right to pursue any, and all, legal and civil action in connection with any such violation.

Any vendor, consultant, or contractor found to have violated this Policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

6. Acknowledgement

Those in receipt of this Policy acknowledge its receipt and understanding of its contents; and that New Era Technology expressly reserves the right to change, modify, or delete its provisions without notice.

Document Information

Reference	Security Framework
Title	Encryption Policy
Purpose	The purpose of the New Era Technology Encryption Policy is to establish the rules for acceptable use of encryption technologies relating to New Era Technology Information Resources.
Owner	Governance, Risk & Compliance (GRC)
Document Approvers	Chief Technology Officer (CTO) Director of Governance, Risk & Compliance (GRC)
Intended Audience	New Era Technology permanent, temporary, and contracted staff responsible for setting up or maintaining New Era Technology encryption technology.
Review Plan	Annually
Document Classification	Public

Document History

VERSION CONTROL

Revision	Date	Record of Changes	Approved /Released By
V1.0	Aug 16, 2022	Approved release	CTO, Dir GRC
V1.1	Aug 9, 2023	Review	Dir GRC
V2.0	Sep 17, 2023	Annual review, classification & approvers update	CTO, Dir GRC
V3.0	Oct 4, 2024	Annual review, updates to sections 2-6	Dir GRC, SVP Corp A&E
V3.0	Oct 18, 2024	Approved release	CTO, Dir GRC

Control of Hardcopy Versions

The digital version of this document is the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. The printed version of this document is uncontrolled, and cannot be relied upon, except when formally issued by the Director of Governance, Risk and Compliance and /or the Chief Technology Officer and provided with a document reference number and revision in the fields below:

Document Ref.	**Rev.**	**Uncontrolled Copy**	**X**	**Controlled Copy**

References

Standard / Framework / Other	Title	Description
New Era GRC Policy	Security Policy	Policy to (a) protect New Era Technology and its customers' data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.
New Era GRC Policy	Acceptable Use Policy	Policy to establish acceptable practices regarding the use of New Era Technology Information Resources to protect the confidentiality, integrity, and availability of information created, collected, and maintained. Inappropriate use exposes New Era to risks, including virus attacks, loss of confidential data, compromise of network systems and services, and legal issues.
New Era GRC Policy	Identity and Access Management (IAM) Policy	Policy to establish the requirements necessary to ensure that access to and use of New Era Technology Information Resources is managed in accordance with business requirements, information security requirements, and other New Era Technology policies and procedures.
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements	Requirements to meet the Standard.
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations	Catalog of security and privacy controls for information systems and organizations.